

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1-24. (Canceled).

Sub C17
1 25. (Currently amended) A method for managing encryption within a
2 database system, wherein encryption is performed automatically and transparently
3 to a user of the database system, the method comprising:
4 receiving a request at the database system to store data in the database
5 system;
6 wherein the request is directed to storing data in a portion of the database
7 system that has been designated as encrypted;
8 in response to receiving the request:
9 ~~creating a digest of the data, and~~
10 automatically encrypting data within the database system
11 using an encryption function to produce an encrypted data; and
12 storing the encrypted data in the database system;
13 ~~wherein the digest is used to detect tampering with the encrypted data.~~

1 26. (Previously presented) The method of claim 25,
2 wherein the portion of the database system that has been designated as
3 encrypted includes a column of the database system;
4 wherein the encryption function uses a key stored in a keyfile managed by
5 a security administrator; and

6 wherein the encrypted data is stored using a storage function of the
7 database system.

1 27. (Previously presented) The method of claim 26, further comprising:
2 receiving a request to retrieve data from the column of the database
3 system;
4 if the request to retrieve data is received from a database administrator,
5 preventing the database administrator from decrypting the encrypted data;
6 if the request to retrieve data is received from the security administrator,
7 preventing the security administrator from decrypting the encrypted data; and
8 if the request to retrieve data is from an authorized user of the database
9 system, allowing the authorized user to decrypt the encrypted data.

1 28. (Previously presented) The method of claim 26, wherein the security
2 administrator selects one of, data encryption standard (DES) and triple DES as a
3 mode of encryption for the column.

1 29. (Previously presented) The method of claim 26, wherein the security
2 administrator, a database administrator, and a user administrator are distinct roles,
3 and wherein a person selected for one of these roles is not allowed to be selected
4 for another of these roles.

1 30. (Previously presented) The method of claim 26, wherein managing the
2 keyfile includes, but is not limited to:
3 creating the keyfile;
4 establishing a plurality of keys to be stored in the keyfile;
5 establishing a relationship between a key identifier and the key stored in
6 the keyfile;

7 storing the keyfile in one of,
8 an encrypted file in the database system, and
9 a location separate from the database system; and
10 moving an obfuscated copy of the keyfile to a volatile memory within a
11 server associated with the database system.

1 31. (Previously presented) The method of claim 30, wherein the key
2 identifier associated with the column is stored as metadata associated with a table
3 containing the column within the database system.

1 32. (Previously presented) The method of claim 30, further comprising
2 establishing encryption parameters for the column, wherein encryption parameters
3 include encryption mode, key length, and integrity type by:
4 entering encryption parameters for the column manually; and
5 recovering encryption parameters for the column from a profile table in the
6 database system.

1 33. (Previously presented) The method of claim 26, wherein upon
2 receiving a request from the security administrator specifying the column to be
3 encrypted, if the column currently contains data, the method further comprises:
4 decrypting the column using an old key if the column was previously
5 encrypted; and
6 encrypting the column using a new key.

1 34. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer causes the computer to perform a
3 method for managing encryption within a database system, wherein encryption is

4 performed automatically and transparently to a user of the database system, the
5 method comprising:
6 receiving a request at the database system to store data in the database
7 system;
8 wherein the request is directed to storing data in a portion of the database
9 system that has been designated as encrypted;
10 in response to receiving the request:
11 , creating a digest of the data, and
12 automatically encrypting data within the database system
13 using an encryption function to produce an encrypted data; and
14 storing the encrypted data in the database system;
15 wherein the digest is used to detect tampering with the encrypted data.

31
1 35. (Previously presented) The computer-readable storage medium of
2 claim 34,
3 wherein the portion of the database system that has been designated as
4 encrypted includes a column of the database system;
5 wherein the encryption function uses a key stored in a keyfile managed by
6 a security administrator; and
7 wherein the encrypted data is stored using a storage function of the
8 database system.

1 36. (Previously presented) The computer-readable storage medium of
2 claim 35, the method
3 further comprising:
4 receiving a request to retrieve data from the column of the database
5 system;

6 if the request to retrieve data is received from a database administrator,
7 preventing the database administrator from decrypting the encrypted data;
8 if the request to retrieve data is received from the security administrator,
9 preventing the security administrator from decrypting the encrypted data; and
10 if the request to retrieve data is from an authorized user of the database
11 system, allowing the authorized user to decrypt the encrypted data.

1 37. (Previously presented) The computer-readable storage medium of
2 claim 35, wherein the security administrator selects one of, data encryption
3 standard (DES) and triple DES as a mode of encryption for the column.

1 38. (Previously presented) The computer-readable storage medium of
2 claim 35, wherein the security administrator, a database administrator, and a user
3 administrator are distinct roles, and wherein a person selected for one of these
4 roles is not allowed to be selected for another of these roles.

31
1 39. (Previously presented) The computer-readable storage medium of
2 claim 35, wherein managing the keyfile includes, but is not limited to:
3 creating the keyfile;
4 establishing a plurality of keys to be stored in the keyfile;
5 establishing a relationship between a key identifier and the key stored in
6 the keyfile;
7 storing the keyfile in one of,
8 an encrypted file in the database system, and
9 a location separate from the database system; and
10 moving an obfuscated copy of the keyfile to a volatile memory within a
11 server associated with the database system.

1 40. (Previously presented) The computer-readable storage medium of
2 claim 39, wherein the key identifier associated with the column is stored as
3 metadata associated with a table containing the column within the database
4 system.

1 41. (Previously presented) The computer-readable storage medium of
2 claim 39, wherein the method further comprises establishing encryption
3 parameters for the column, wherein encryption parameters include encryption
4 mode, key length, and integrity type by:
5 entering encryption parameters for the column manually; and
6 recovering encryption parameters for the column from a profile table in the
7 database system.

1 42. (Previously presented) The computer-readable storage medium of
2 claim 35, wherein upon receiving a request from the security administrator
3 specifying the column to be encrypted, if the column currently contains data, the
4 method further comprises:

5 decrypting the column using an old key if the column was previously
6 encrypted; and
7 encrypting the column using a new key.

1 43. (Currently amended) An apparatus that facilitates managing encryption
2 within a database system, wherein encryption is performed automatically and
3 transparently to a user of the database system, comprising:
4 a receiving mechanism that is configured to receive a request at the
5 database system to store data in the database system;
6 wherein the request is directed to storing data in a portion of the database
7 system that has been designated as encrypted;

8 | a digest creating mechanism configured to create a digest of the data;
9 | an encrypting mechanism that is configured to automatically encrypt data
10 | within the database system using an encryption function to produce an encrypted
11 | data; and
12 | a storing mechanism that is configured to store the encrypted data in the
13 | database system;
14 | wherein the digest is used to detect tampering with the encrypted data.

1 | 44. (Previously presented) The apparatus of claim 43,
2 | wherein the portion of the database system that has been designated as
3 | encrypted includes a column of the database system;
4 | wherein the encryption function uses a key stored in a keyfile managed by
5 | a security administrator; and
6 | wherein the encrypted data is stored using a storage function of the
7 | database system.

1 | 45. (Previously presented) The apparatus of claim 44, further comprising:
2 | the receiving mechanism that is further configured to receive a request to
3 | retrieve data from the column of the database system;
4 | an access mechanism that is configured to prevent a database administrator
5 | and the security administrator from decrypting the encrypted data; and
6 | wherein the access mechanism is configured to allow an authorized user
7 | of the database system to decrypt the encrypted data.

1 | 46. (Previously presented) The apparatus of claim 44, further comprising a
2 | selection mechanism that is configured to select one of, data encryption standard
3 | (DES) and triple DES as a mode of encryption for the column.

1 47. (Previously presented) The apparatus of claim 44, wherein the security
2 administrator, a database administrator, and a user administrator are distinct roles,
3 and wherein a person selected for one of these roles is not allowed to be selected
4 for another of these roles.

1 48. (Previously presented) The apparatus of claim 44, further comprising:
2 a creating mechanism that is configured to create the keyfile;
3 an establishing mechanism that is configured to establish a plurality of
4 keys to be stored in the keyfile;
5 wherein the establishing mechanism is further configured to establish a
6 relationship between a key identifier and the key stored in the keyfile;
7 wherein the storing mechanism is further configured to store the keyfile in
8 one of,
9 an encrypted file in the database system, and
10 a location separate from the database system; and
11 a moving mechanism that is configured to move an obfuscated copy of the
12 keyfile to a volatile memory within a server associated with the database system.

1 49. (Previously presented) The apparatus of claim 48, wherein the key
2 identifier associated with the column is stored as metadata associated with a table
3 containing the column within the database system.

1 50. (Previously presented) apparatus of claim 48, wherein the
2 establishing mechanism is further configured to establish encryption parameters
3 for the column, wherein encryption parameters include encryption mode, key
4 length, and integrity type, and wherein the establishing mechanism includes:
5 an entering mechanism that is configured to enter encryption parameters
6 for the column manually; and

7 a recovering mechanism that is configured to recover encryption
8 parameters for the column from a profile table in the database system.

1 51. (Previously presented) The apparatus of claim 44, further comprising:
2 a decrypting mechanism that is configured to decrypt the column using a
3 previous key if the column was previously encrypted; and
4 wherein the encrypting mechanism is further configured to encrypt the
5 column using a new key.

31